



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



Publication number:

**0 427 465 A3**

(12)

## EUROPEAN PATENT APPLICATION

(21) Application number: 90312005.3

(51) Int. Cl.<sup>5</sup>: G07F 7/10, G07C 9/00,  
G06F 1/00

(22) Date of filing: 01.11.90

(30) Priority: 09.11.89 US 433821

(43) Date of publication of application:  
15.05.91 Bulletin 91/20

(84) Designated Contracting States:  
DE FR GB IT

(88) Date of deferred publication of the search report:  
24.07.91 Bulletin 91/30

(71) Applicant: **AMERICAN TELEPHONE AND  
TELEGRAPH COMPANY**  
550 Madison Avenue  
New York, NY 10022(US)

(72) Inventor: **Claus, David Michael**  
7660 Brookview Lane  
Indianapolis, Indiana 46250(US)

Inventor: **Coutinho, Roy S.**  
10905 Timber Lane  
Carmel, Indiana 46032(US)  
Inventor: **Murphy, Kevin Dean**  
6021 Middle Drive  
Indianapolis, Indiana 46236(US)  
Inventor: **Snavley, James Damon**  
262 North Brewer Street  
Greenwood, Indiana 46142(US)  
Inventor: **Zempol, Kenneth Robert**  
44 Center Grove Road, Apt. F26  
Randolph, New Jersey 07920(US)

(74) Representative: **Watts, Christopher Malcolm  
Kelway et al**  
AT&T (UK) LTD. AT&T Intellectual Property  
Division 5 Mornington Road  
Woodford Green Essex IG8 OTU(GB)

(54) Databaseless security system.

(57) An improved security system, including a portable smart card (500) and a host computer (600), eliminates the need for the computer to store individual personal identification (ID) numbers for each user seeking access to the computer. Instead, the computer stores a first encryption algorithm  $E_1$  used in converting a particular identification number  $(ID)_n$  into a secret code  $S_n$  for that particular user.  $S_n$  also exists within the memory of the smart card having been loaded into its memory at the time of issue. A challenge number  $C$  is generated by the computer and transmitted to the smart card. Within the smart card and the computer, microprocessors respond to the challenge number  $C$ , the secret code  $S_n$ , and a second encryption algorithm  $E_2$  in order to generate response numbers  $R_n$  and  $R'_n$  respectively. Thereafter,  $R_n$  is transmitted to the computer where it is compared with  $R'_n$ . A favorable comparison is necessary for gaining access to the computer.

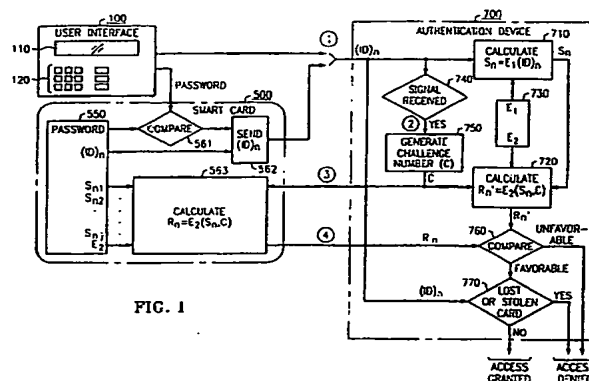


FIG. 1

EP 0 427 465 A3



European  
Patent Office

## EUROPEAN SEARCH REPORT

Application Number

EP 90 31 2005

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A	EP-A-0 029 894 (IBM) * abstract; claim 1 * - - - -	1,9	G 07 F 7/10 G 07 C 9/00 G 06 F 1/00
A	EP-A-0 131 421 (AMERICAN TELEPHONE AND TELEGRAPH COMPANY) * abstract * - - - -	1,9	
A	EP-A-0 281 059 (SIEMENS) * abstract * - - - -	1,9	
A	US-A-4 310 720 (CHECK) * abstract * - - - -	1,9	
A	EP-A-0 114 773 (CII HONEYWELL BULL) * abstract * - - - -	1,9	
A	EP-A-0 281 058 (SIEMENS) * abstract * - - - -	1,9	
A	EP-A-0 284 133 (TRT) * claim 1 * - - - -	1,9	
D,A	US-A-4 453 074 (WEINSTEIN) - - - -		
D,A	US-A-4 471 216 (HERVE) * abstract * - - - - -	1,9	
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of search 30 May 91	Examiner TACCOEN J-F.P.L.
<div>CATEGORY OF CITED DOCUMENTS</div> <div>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention</div> <div>E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons &amp; : member of the same patent family, corresponding document</div>			